PA-500

The PA-500 is a next-generation firewall that delivers unprecedented visibility and control over applications, users and content on enterprise networks.

APPLICATION IDENTIFICATION:

- Identifies more than 950 applications irrespective of port, protocol, SSL encryption or evasive tactic employed.
- Enables positive enforcement application usage policies: allow, deny, schedule, inspect, apply traffic shaping.
- Graphical visibility tools enable simple and intuitive view into application traffic.

USER IDENTIFICATION:

- Policy-based visibility and control over who is using the applications through seamless integration with Active Directory, LDAP, and eDirectory.
- Identifies Citrix and Microsoft Terminal Services users, enabling visibility and control over their respective application usage.
- Control non-Windows hosts via web-based authentication.

CONTENT IDENTIFICATION:

- Block viruses, spyware, and vulnerability exploits, limit unauthorized transfer of files and sensitive data such as CC# or SSN, and control non-work related web surfing.
- Single pass software architecture enables multi-gigabit throughput with low latency while scanning content.

PA-500

The Palo Alto Networks™ PA-500 is targeted at high speed Internet gateway deployments for enterprise branch offices and medium size businesses. The PA-500 manages network traffic flows using dedicated computing resources for networking, security, threat prevention and management.

A high speed backplane smoothes the pathway between processors and the separation of data and control plane ensures that management access is always available, irrespective of the traffic load. Interface density for the PA-500 includes (8) 10/100/1000 traffic interfaces and a dedicated out-of-band management interface.

The controlling element of the PA-500 Series next-generation firewalls is PAN-OS™, a security-specific operating system that tightly integrates three unique identification technologies: App-ID™, User-ID and Content-ID, with key firewall, networking and management features.

KEY PERFORMANCE SPECIFICATIONS	PA-500
Firewall throughput	250 Mbps
Threat prevention throughput	100 Mbps
IPSec VPN throughput	50 Mbps
IPSec VPN tunnels/tunnel interfaces	250
SSL VPN concurrent users	100
New sessions per second	7,500
Max sessions	64,000

For a complete description of the PA-500 next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

paloalto NETWORKS

Additional PA-500 Features and Specifications

APP-ID

- Identifies and controls more than 950 applications
- SSL decryption (inbound and outbound)
- Customize application properties
- Custom HTTP and SSL applications

FIREWALL

- Policy-based control by application, application category, subcategory, technology, risk factor or characteristic
- Application function control
- Fragmented packet protection
- Reconnaissance scan protection
- Denial of Service (DoS)/Distributed Denial of Services (DDoS) protection
- Maximum number of policies: 1,000

USER-ID

- Visibility and control by user, group and IP address
- Active Directory, LDAP, eDirectory, Citrix and Microsoft Terminal Services
- XML API (external user repository integration)
- WMI and NetBios polling
- Maximum concurrent user/IP mappings: 64,000

DATA FILTERING

- Control unauthorized data transfer (social security numbers, credit card numbers, custom data patterns)
- Control unauthorized transfer of more than 50 file types

URL FILTERING (SUBSCRIPTION REQUIRED)

- 76-category, 20M URL on-box database
- Custom 1M URL cache database (from 180M URL database)
- Custom block pages and URL categories

IPSEC VPN (SITE-TO-SITE)

- Manual key, IKE v1
- 3DES, AES (128-bit, 192-bit, 256-bit) encryption
- SHA1, MD5 authentication

SSL VPN (REMOTE ACCESS)

- IPSec transport with SSL fall-back
- Enforce unique policies for SSL VPN traffic
- Enable/disable split tunneling to control client access
- LDAP, SecurID, or local DB authentication
- Client OS: Windows XP, Windows Vista (32 and 64 bit), Windows 7 (32 and 64 bit)

HIGH AVAILABILITY

- Active/Passive failover
- Configuration and session synchronization
- Heartbeat checking
- Link and path failure monitoring

NETWORKING

- Dynamic routing (BGP, OSPF and RIPv2)
- Tap mode, virtual wire, layer 2, layer 3
- Network address translation (NAT)
  - Source and destination address translation
  - Dynamic IP and port pool: 254
  - Dynamic IP pool: 16,234
- DHCP server/ DHCP relay: Up to 3 servers
- 802.1Q VLANs: 4,094
- Policy-based forwarding
- Point-to-Point Protocol over Ethernet (PPPoE)
- IPv6 application visibility, control and full content inspection (Virtual wire mode only)
- Security zones: 20
- Virtual routers: 3

THREAT PREVENTION (SUBSCRIPTION REQUIRED)

- Detect and block application vulnerability exploits (IPS)
- Stream-based protection against viruses, spyware and worms
- HTML/Javascript virus protection
- Inspect compressed files that use the Deflate algorithm (Zip, Gzip, etc)
- Custom vulnerability and spyware phone home signatures
- Content updates: daily (malware), weekly (vulnerability signatures), emergency (all)

QUALITY OF SERVICE (QOS)

- Policy-based traffic shaping by application, user, source, destination, interface, IPSec VPN tunnel and more
- 8 traffic classes with guaranteed, maximum and priority bandwidth parameters
- Real-time bandwidth monitor
- Per policy diffserv marking

MANAGEMENT TOOLS

- Integrated web interface
- Command line interface (CLI)
- Role-based administration
- Syslog and SNMPv2
- Customizable administrator login banner
- XML-based REST API
- Centralized management (Panorama)
- Centrally manage PAN-OS and content updates (Panorama)
- Shared policies (Panorama)

VISIBILITY AND REPORTING TOOLS

- Graphical summary of applications, URL categories, threats and data (ACC)
- View, filter, export traffic, threat, URL, and data filtering logs
- Fully customizable reporting
- Trace session tool

HARDWARE SPECIFICATIONS

I/O	(8) 10/100/1000
Management I/O	(1) 10/100/1000 out-of-band management port, (1) RJ-45 console port
Power supply (Avg/max power consumption)	180W (10W/75W)
Input voltage (Input frequency)	100-240Vac (50-60Hz)
Power factor	0.997 to 0.978
Max input current	110A@230Vac; 1A@115Vac
Rack mountable (Dimensions)	1U, 19" standard rack (1.75"H x 10"D x 17"W)
Safety	UL, CUL, CB
EMI	FCC Class A, CE Class A, VCCI Class A, TUV
MTBF	10.16 years

ENVIRONMENT

Operating temperature	32° to 122° F, 0° to 50° C
Non-operating temperature	-4° to 158° F, -20° to 70° C

ORDERING INFORMATION	PA-500
Platform	PAN-PA-500
Annual threat prevention subscription	PAN-PA-500-TP
Annual URL filtering subscription	PAN-PA-500-URL2

For additional Information on the PA-500 next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA. 94089
Sales 866.320.4788
408.738.7700
www.paloaltonetworks.com

840-000009-00B